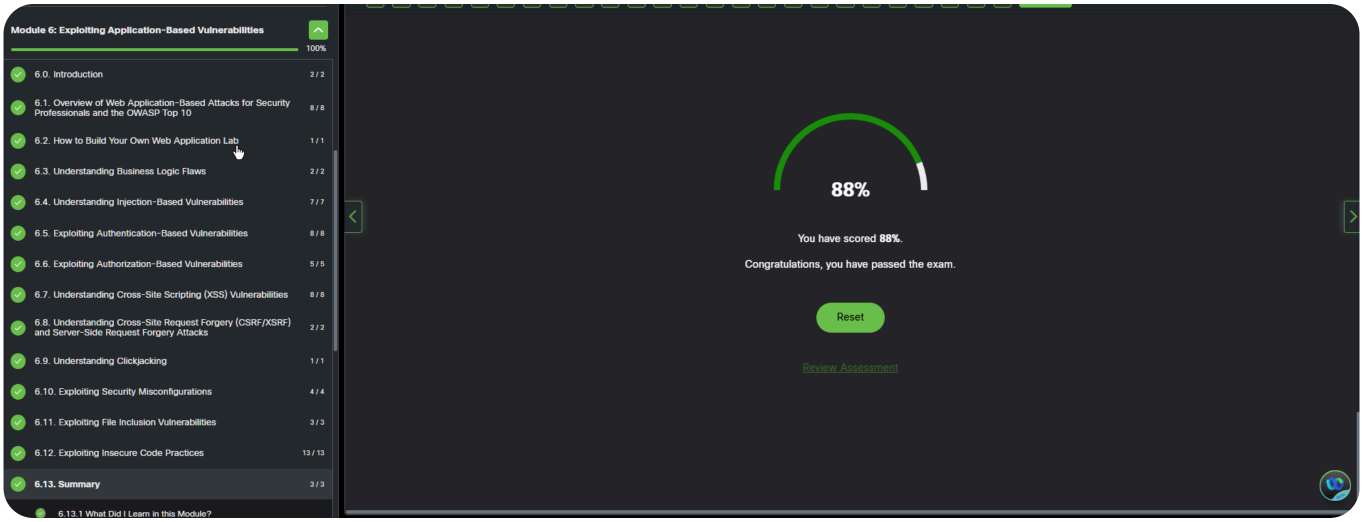
Ethical Hacking -- Week 4 -- Assignment 1

Screenshots



Module 6: Exploiting Application-Based Vulnerabilities 100%

6.0. Introduction	2 / 2
6.1. Overview of Web Application-Based Attacks for Security Professionals and the OWASP Top 10	8 / 8
6.2. How to Build Your Own Web Application Lab	1 / 1
6.3. Understanding Business Logic Flaws	2 / 2
6.4. Understanding Injection-Based Vulnerabilities	7 / 7
6.5. Exploiting Authentication-Based Vulnerabilities	8 / 8
6.6. Exploiting Authorization-Based Vulnerabilities	5 / 5
6.7. Understanding Cross-Site Scripting (XSS) Vulnerabilities	8 / 8
6.8. Understanding Cross-Site Request Forgery (CSRF/XSRF) and Server-Side Request Forgery Attacks	2 / 2
6.9. Understanding Clickjacking	1 / 1
6.10. Exploiting Security Misconfigurations	4 / 4
6.11. Exploiting File Inclusion Vulnerabilities	3 / 3
6.12. Exploiting Insecure Code Practices	13 / 13
6.13. Summary	3 / 3
6.13.1 What Did I Learn in this Module?	

88%

You have scored **88%**.

Congratulations, you have passed the exam.

Labs

6.1.7 – Website Vulnerability Scanning

- I used Nikto to uncover SQL injection vulnerabilities
  - Can test multiple web servers by putting a list of addresses in a text file
- Nikto gives information about the vulnerabilities it uncovered for me
  - some in the Open Source Vulnerability Database (OSVDB), the Common Weakness Enumeration (CWE), or the Common Vulnerabilities and Exposures (CVE)
- exported results to a csv so that it is formatted nicely and easily readable and highly compatible

6.1.8 – Using the GVM Vulnerability Scanner

- used gvm tool to scan Metasploitable host
- started with GUI
  - scan took forever
- GUI is nice can click into the scan after it is done and easily analyze the data that was exported for me
  - listed in order of severity
- rexec and SMB ports were open, so exploitable
- logging into the target using rsh (remote shell)

    - able to obtain root access, full elevated control

6.4.7 – Injection Attack

- navigated to the DVWA site to set the security policy to “Low”
    - allows to test for SQL injection
- using apostrophe at beginning of query can test for returned errors, meaning that SQL injection may be possible
- used commands to poke and prod, incrementing the order by one until you get an error
    - tells you how many fields are availabel in the query
- used SQL injection to find the method used for database management

```
1' OR 1=1 UNION SELECT 1, VERSION()#
```

- SQL injection to determine database name

```
1' OR 1=1 UNION SELECT 1, DATABASE()#
```

- retrieved the table names

```
1' OR 1=1 UNION SELECT 1,table_name FROM information_schema.tables WHERE
table_type='base table' AND table_schema='dvwa'#
```

- returned users and guestbook, but we wanna get into the users table to potentially access usernames and password hashes

```
1' OR 1=1 UNION SELECT user, password FROM users #
```

- was able to find admin credentials
    - admin
    - password
- also pablo
    - pablo
    - letmein
        - who are you, Eric Andre?

6.5.8 – Using Password Tools

- discovered some new tools in Kali for password attacks

    - ophcrack-cli is one that uses rainbow tables
    - the lab wanted me to install rainbowcrack, but that is no longer available in the kali repositories
- used hashcat and wordlists against discovered hashes in order to potentially crack passwords
- john ripper tool was a little more fun, mostly because of the name
    - when unable to crack hashes with wordlists, begins brute forcing (slowwww)

6.7.8 – Cross Site Scripting

- logged into DVWA and explored the menus on the left
    - XSS (Reflected) in order to create an alert
- looking through the source code we can see that it replaces the string `<script>` with NULL, but it doesn’t check for different cases
    - `<ScRiPt>` was able to bypass this
- at high security,

```
**$name = preg_replace( '/<(.*)s(.*)c(.*)r(.*)i(.*)p(.*)t/i', '', $_GET[
'name' ] );**
```

- wildcards make it much harder to get around
    - can use different HTML tag

```
<img src=x onerror=alert("You are hacked!")>
```

- creates alert, but as an image